IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER (Large Entity)

Application Number: **09/739,844** Group Art Unit: **2151**

Filed: **December 20, 2000** Examiner Name: **Phillips, Hassan A.**

Applicant: **BONEFAS** Attorney Docket Number: **20-565**

TITLE: **A MESSAGING METHOD AND APPARATUS FOR ROUTING MESSAGES IN A CLIENT SERVER ENVIRONMENT OVER MULTIPLE WIRELESS AND WIRELINE NETWORKS**

Total Number of Pages in this Submission: 3 X 33 (In Triplicate)

COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

SIR:

Transmitted herewith is
an Appeal Brief in the above-identified application (33 Pages)

The fee has been calculated and is transmitted as shown below.

CLAIMS AS AMENDED					
	CLAIMS REMAINING AFTER Amendment	HIGHEST # PREV. PAID FOR	# OF EXTRA CLAIMS	RATE	ADDITIONAL FEE
Total Claims	41	41	0	x $50 =	$ 0.00
Independent Claims	10	10	0	x $100 =	$ 0.00
Appeal Brief Fee				x $500=	$ 500.00
		TOTAL ADDITIONAL FEE:			$500.00

The Commissioner is hereby authorized to charge any additional fees required under 37 C.F.R. 1.16 or any patent application processing fees under 37 C.F.R. 1.17 associated with this communication, or credit any over payment to **Deposit Account No. 50-0687 under Order No. 20-565.**

Respectfully submitted,

(#46,504)

William H. Bollman
Reg. No.: 36,457
Attorney for Applicant(s)

Date: January 21, 2005
Manelli Denison & Selter PLLC
2000 M Street, NW Suite 700
Washington, DC 20036-3307
(202) 261-1020

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Serial No.: **09/739,844**
Filed: **December 20, 2000**
Group Art Unit: **2151**
Examiner: **Phillips, Hassan**
Attorney Docket No.: **20-565**

IN RE PATENT APPLICATION OF:

BONEFAS ET AL.

TITLE: A MESSAGING METHOD AND APPARATUS FOR ROUTING MESSAGES IN A CLIENT SERVER ENVIRONMENT OVER MULTIPLE WIRELESS AND WIRELINE NETWORKS

January 21, 2005

APPEAL BRIEF

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The Applicants submit herewith the following Appeal Brief in triplicate as required by 37 C.F.R. § 1.192.

(1) REAL PARTY IN INTEREST

The real party in interest is TeleCommunication Systems, Inc.

(2) RELATED APPEALS AND INTERFERENCES

The Applicants and their legal representatives and assignee are not aware of any other appeals or interferences that will directly affect or be directly affected by or have a bearing on the Board's decision in the appending Appeal.

01/25/2005 MAHMED1 00000051 09739844
01 FC:1402 500.00 OP

(3) STATUS OF THE CLAIMS

Claims 1-41 are pending in this application. Claims 1-41 stand rejected.

(4) STATUS OF ANY AMENDMENT FILED SUBSEQUENT TO FINAL REJECTION

The Applicants filed amendments to claims 34 and 36 in an After Final response filed October 4, 2004. The Examiner indicated in the Advisory Action dated November 22, 2004 that the amendments to claims 34 and 36 have been entered and corrected any outstanding objections and 35 USC 112 rejections.

(5) SUMMARY OF THE INVENTION

The present invention is directed to an apparatus and method of allowing two devices to specify how they communicate with one another on a level-to-level basis, rather than having to negotiate one giant protocol for the entire network. This means that logical communications can occur at the peer protocol layer.

Messages transmitted over the network that exceed a predefined segment size can be segmented into multiple message segments. Upon receipt of the message segments, the message segments are assembled into a complete message, acknowledgement of the entire message being sent after assembly of the complete message.

A protocol gateway facilitates upgradeability within the system by providing the flexibility to support multiple present and future access protocols. This upgradeability can be accomplished by remote access. The protocol gateway is part of an intelligent messaging network that can provide network transparency to developers of client and server applications. As such, developers do not need to concern themselves with implementation details of the underlying network protocols or with various platform specific encoding such as, e.g., big-endian and little-endian.

(6) CONCISE STATEMENT OF THE ISSUES PRESENTED FOR REVIEW

(A) Whether claims 1-4, 19, 22-24, 27-29, 32 and 33 are obvious under 35 U.S.C. §103(a) over U.S. Patent No. 6,507,589 to Ramasubramani et al. ("Ramasubramani") in view of U.S. Patent No. 6,138,158 to Boyle et al. ("Boyle").

(B) Whether claims 5, 34 and 35 are obvious under 35 U.S.C. §103(a) over Ramasubramani in view of U.S. Patent No. 6,012,100 to Frailong et al. ("Frailong").

(C) Whether claims 6-11 are obvious under 35 U.S.C. §103(a) over Ramasubramani in view of Frailong, and further in view of Boyle.

(D) Whether claims 12-18 are obvious under 35 U.S.C. §103(a) over Ramasubramani in view of U.S. Patent No. 5,167,035 to Mann et al. ("Mann").

(E) Whether claims 20, 21, 25, 26, 30 and 31 are obvious under 35 U.S.C. §103(a) over Ramasubramani in view of Boyle, and further in view of U.S. Patent No. 5,371,852 to Attanasio ("Attanasio").

(F) Whether claims 36-41 are obvious under 35 U.S.C. §103(a) over Mann in view of Ramasubramani.

(7) WHETHER THE CLAIMS STAND OR FALL TOGETHER

Group I: Claims 1-4 and 19-33 stand or fall together because each includes the following distinctive features:

(1) a method of routing and a message router authenticating an origin of a message before the message is routed by the message router between a protocol gateway and a server;

(2) a database accessible by the message router; and

(3) storing information relating to routing and authentication of the message.

Group III: Claims 5-11, 34 and 35 stand or fall together because each includes the following distinctive feature:

(1) remotely manageable protocol gateway.

Group III: Claims 12-18 and 36-38 stand or fall together because each includes the following distinctive features:

(1) segmenting a message into one or more message segments by a client device, none of the message segments exceeding a maximum segment size;

(2) determining that at least one message segment constitutes a complete message by the client device; and

(3) if the message segment constitutes a complete message as determined the client device, transmitting from a protocol gateway to a message router the complete message.

Group IV: Claims 39-41 stand or fall together because each includes the following distinctive features:

(1) segmenting a message into one or more message segments by a protocol gateway, none of the message segments exceeding a maximum segment size; and

(2) determining by a client device that the message segment constitutes a complete message.

(8) ARGUMENTS WITH RESPECT TO THE ISSUES PRESENTED FOR REVIEW

(A) Claims 1-4, 19, 22-24, 27-29, 32 and 33 are not obvious under 35 U.S.C. § 103(a) over Ramasubramani in view of Boyle.

Claims 1-4, 19, 22-24, 27-29, 32 and 33 require a method of routing and a message router authenticating an origin of a message before the message is routed by the message router between a protocol gateway and a server, a database accessible by the message router, and storing information relating to routing and authentication of the message.

The Examiner acknowledges that Ramasubramani fails to disclose authenticating an origin of a message before the message is routed, and a database relating to the routing and authentication of the message (See Office

Action dated August 4, 2004, pages 8 and 24). The Examiner relies on Boyle at at col. 14, lines 21-34; col. 9, lines 1-2 and col. 8, lines 52-67 to allegedly make up for the deficiencies in Ramasubramani (See Office Action dated August 4, 2004, pages 8 and 25). The Applicants respectfully disagree.

Boyle **fails** to disclose authenticating the original of a message. Boyle simply checks to see if a request for an update ID matches an ID in a local database to **authenticate a mobile device's access to an update** (See Boyle at col. 14, lines 21-34). Boyle fails to determine if an indicated origin of a message actually sent the message, i.e., to authenticate the origin of a message, as recited by claims 1-4, 19, 22-24, 27-29, 32 and 33.

Moreover, Boyle discloses a system and method of allowing a mobile device more efficiently obtaining Internet Web pages by only obtaining updates when such updates are available, facilitated by a link server (See Boyle, Abstract; Fig. 2). Boyle fails to disclose or suggest use of a protocol gateway. Ramasubramani theoretically modified by the disclosure of Boyle would still result in Ramasubramani's protocol gateway working in conjunction with Boyle's link server device checking a device ID requesting an update to an ID stored in a local database to authenticate a mobile device's access to a database. Theoretically modifying Ramasubramani with the disclosure of Boyle would still fail to disclose or suggest a message router routing a message between a protocol gateway and a server, much less a method of routing and a message router authenticating an origin of a message before the message is routed by the message router between a protocol gateway and a server, a database accessible by the message router, and storing information relating to routing and authentication of the message, as recited by claims 1-4, 19, 22-24, 27-29, 32 and 33.

Moreover, the Examiner provides general motivation of why one of ordinary skill in the art would authenticate the origin of a message, but has still failed to provide motivation why one of ordinary skill in the art would have modified Ramasubramani's protocol gateway to perform such a function.

The Examiner alleges that Boyle is relied on to "merely show that authenticating the origin of messages was well known in the art at the time of the invention, and thus, given the teachings of Boyle, it would have been obvious to a person of ordinary skill in the art, at the time of the invention, to modify the teachings of Ramasubramani in order to show the protocol gateway taught by Ramasubramani ...would have verified the integrity of the message by ensuring that the message is valid, authorized, and unaltered, before establishing communication message" (See Office Action dated August 4, 2004, page 4). The Examiner points to Boyle, col. 2, lines 29-56 for support of such an allegation (See Office Action dated August 4, 2004, page 4).

Boyle discloses a link server device that utilizes a device ID to obtain updates. Boyle fails to even mention use of a protocol gateway or a message router. The Examiner is taking the disclosure of Boyle out of context. The Examiner potentially may be able to find numerous references disclosing authenticating the origin of messages (although the Examiner has failed to provide a single reference), the Applicants are not disputing such. However, the Applicants are **NOT** claiming just any method and device authenticating the origin of messages, but **specifically** a method of routing and a message router. Since Applicants' method of routing and message router and Boyle's link server are two completely different methods and devices performing completely different functions, the Examiner has still failed to provide a single reference that discloses or suggests a method of routing and a message router authenticating the origin of messages and/or modifying a message router that routes a message between a protocol gateway and a server to authenticate the origin of messages.

Moreover, even if Boyle is relied on to disclose authenticating the origin of a message (which as discussed above Boyle fails to disclose), "Teachings of references can be combined only if there is some suggestion or incentive to do so." In re Fine, 5 USPQ2d 1596,1600 (Fed. Cir. 1988) (quoting ACS Hosp. Sys. v. Montefiore Hosp., 221 USPQ 929, 933 (Fed. Cir. 1984)) (emphasis in original). The Examiner has not provided motivation why one of ordinary skill in the art would modify Ramasubramani to authenticating the origin

of a message, much less modify Ramasubramani with a message router to authenticating the origin of a message. Ramasubramani fails to disclose or suggest any type of need to be modified to authenticate the origin of a message. Thus, modification of Ramasubramani would not cure any deficiencies that would benefit Ramasubramani's invention from the alleged modification.

Moreover, the Examiner alleges the motivation to authenticate the origin of a message is to "verify the integrity of the message by ensuring that the message is valid, authorized, and unaltered, before establishing a communication message" (See Office Action dated August 4, 2004, page 4). However, authenticating the origin of the message would **not ensure** that the message is valid, authorized and unaltered. During the course of transmission, the message could have been invalidated and altered but still be validated as coming from a particular origin. A message containing origin information does not automatically indicate the message is authorized. Thus, **none** of the Examiner purposes to authenticate the origin of a message would fulfill the Examiner's allegations, much less fulfill some type of need in Ramasubramani to perform such authentication.

It is respectfully submitted that not only does this rejection fail on its face, and thus is improper, but also in light of the above comments its clear that Ramasubramani in view of Boyle does not render obvious any of claims 1-4, 19, 22-24, 27-29, 32 and 33. Thus, the rejection of claims 1-4, 19, 22-24, 27-29, 32 and 33 under 35 U.S.C. § 103(a) is improper and should be reversed.

(B) Claims 5, 34 and 35 are not obvious under 35 U.S.C. § 103(a) over Ramasubramani in view of Failong.

Claims 5, 34 and 35 require a remotely manageable **protocol gateway**.

The Examiner acknowledges that Ramasubramani fails to disclose a **remotely manageable** protocol gateway (See Office Action dated August 4, 2004, page 11). The Examiner relies on Frailong to allegedly make up for the

deficiencies in Ramasubramani to arrive at the claimed features. The Applicants respectfully disagree.

The Examiner relies on Frailong to disclose a gateway being remotely manageable at col. 5, lines 18-34 (See Office Action dated August 4, 204, page 11).

Thus, by the Examiner's own acknowledgement, Frailong fails to make up for the deficiencies in Ramasubramani and fails to disclose a remotely manageable **protocol gateway**, as recited by claims 5, 34 and 35.

Frailong discloses a remotely upgradeable gateway interface device (See col. 5, lines 18-30). Such information includes configuration information related to a LAN, internet address blocks, internet domain names, and data related to physical and interfaces between a client network and an ISP (See Frailong, col. 5, lines 31-34).

Thus, Frailong discloses configuration information related to a LAN, internet address blocks, internet domain names, and data related to physical and interfaces between a client network and an ISP. Frailong fails to managing any device having protocol related functions, much less a remotely manageable **protocol gateway**, as recited by claims 5-11, 34 and 35.

Thus, Ramasubramani modified by the disclosure of Frailong would still fail to disclose, teach or suggest a remotely manageable **protocol gateway**, as recited by 5-11, 34 and 35.

Moreover, the Examiner's motivation to modify the disclosure of Ramasubramani with the disclosure of Frailong is unfounded. The Examiner alleges modifying the disclosure of Ramasubramani with the disclosure of Frailong would minimize the clients responsibilities by configuring and maintaining the protocol gateway remotely (See Office Action dated August 4, 2004, page 11). However, conventionally protocol gateways require a technician, **not** a client, to travel in the field to the protocol gateway to perform any maintenance. A protocol gateway is responsible for, e.g., conversion of protocols between networks, and therefore require updates when protocol updates exist. Frailong fails to disclose a protocol gateway, and therefore would

fail to disclose remotely managing functions specifically related to a protocol gateway.

Moreover as discussed above, "Teachings of references can be combined only if there is some suggestion or incentive to do so." In re Fine, 5 USPQ2d 1596,1600 (Fed. Cir. 1988) (quoting ACS Hosp. Sys. v. Montefiore Hosp., 221 USPQ 929, 933 (Fed. Cir. 1984)) (emphasis in original). The Examiner has not provided any motivation why one of ordinary skill in the art would modify Ramasubramani with the disclosure of Frailong that fails to even mention a protocol gateway. Ramasubramani fails to disclose or suggest any type of need that would benefit from modifying a protocol gateway to be remotely manageable. Thus, modification of Ramasubramani would not cure any disclosed deficiencies that would benefit from the alleged modification and would therefore be based on an improper use of hindsight.

Therefore, Ramasubramani modified by the disclosure of Frailong would fail to disclose, teach or suggest a remotely manageable **protocol gateway** (as acknowledged by the Examiner), nor suggest a **protocol gateway** to be modified to be remotely manageable, as recited by claims 5, 34 and 35.

It is respectfully submitted that not only does this rejection fail on its face, but in view of the above comments its clear that claims 5, 34 and 35 are not rendered obvious over Ramasubramani in view of Frailong. Thus, the rejection of claims 5, 34 and 35 under 35 U.S.C. § 103(a) over Ramasubramani in view of Frailong is improper and should be reversed.

(C) Claims 6-11 are not obvious under 35 U.S.C. § 103(a) over Ramasubramani in view of Frailong and Boyle

Claims 6-11 require a remotely manageable **protocol gateway**.

As discussed above, Ramasubramani in view of Frailong fails to disclose a remotely manageable **protocol gateway** nor suggest modifying a **protocol gateway** to be remotely manageable.

The Office Action relies on Boyle to allegedly make up for the deficiencies in Ramasubramani in view of Frailong to arrive at the claimed features. The Applicants respectfully disagree.

Boyle appears to disclose a link server device that connects a client device and a Web server device (See Fig. 2). The link server services a narrowband channel and a wideband channel connected to a client device (See Boyle, Fig. 2). However, Boyle fails to disclose or suggest that the link server is remotely manageable or performs protocol functions, much less disclose or suggest a remotely manageable **protocol gateway**, as recited by claims 6-11.

Ramasubramani modified by the disclosure of Frailong and Boyle would still fail to disclose or teach a remotely manageable **protocol gateway** and fails to suggest modifying a **protocol gateway** to be remotely mangageable, as recited by 6-11.

It is respectfully submitted that not only does this rejection fail on its face, but in view of the above comments its clear that claims 6-11 are not rendered obvious over Ramasubramani in view of Frailong and Boyle. Thus, the rejection of claims 6-11 under 35 U.S.C. § 103(a) over Ramasubramani in view of Frailong and Boyle is improper and should be reversed.

(D) Claims 12-18 are not obvious under 35 U.S.C. § 103(a) over Ramasubramani in view of Mann.

Claims 12-18 require a method of segmenting a message into one or more message segments by a client device, none of the message segments exceeding a maximum segment size, determining that at least one message segment constitutes a complete message by the client device and if the message segment constitutes a complete message as determined the client device, transmitting from a protocol gateway to a message router the complete message.

The Examiner acknowledges that Ramasubramani fails to disclose segmenting a message into one or more message segments within one of a plurality of client devices, none of the message segments exceeding a maximum segment size and determining that at least one message segment constitutes a

complete message at one of the plurality of client devices (See Office Action dated August 4, 2004, page 15).

The Examiner alleges that Mann is relied on "to merely show that message segmentation was well known in the art at the time of the invention" (See Office Action dated August 4, 2004, page 6). And, "being that client devices, servers, and gateways all have similar functionality, given the teachings of Mann, it would have been obvious to a person of ordinary skill in the art ...to modify the teachings of Ramasubramani in order to .." arrive at the claimed features. The Applicants respectfully disagree.

The Examiner **acknowledges** that Mann fails to disclose segmenting a message by a client device into a maximum segment size (See Office Action dated August 4, 2004, page 6). Thus, neither Ramasubramani nor Mann disclose or suggest segmenting a message by a client device into a maximum segment size, much less none of the message segments exceeding a maximum segment size and determining that at least one message segment constitutes a complete message at one of the plurality of client devices and if the message segment constitutes a complete message as determined the client device, transmitting from a protocol gateway to a message router the complete message, as recited by claims 12-18.

Moreover, the Examiner allegation that client devices, servers, and gateways all have similar functionality is **nonsensical** and unsupported. If client devices, servers, and gateways have similar functionality, then they would all be known within the art as a single term, either a client devices, servers, and gateways. Client devices, servers, and gateways individually perform very specific functions within a data network and are not interchangeable.

Moreover as discussed above, "Teachings of references can be combined only if there is some suggestion or incentive to do so." In re Fine, 5 USPQ2d 1596,1600 (Fed. Cir. 1988) (quoting ACS Hosp. Sys. v. Montefiore Hosp., 221 USPQ 929, 933 (Fed. Cir. 1984)) (emphasis in original). The Examiner has not provided motivation why one of ordinary skill in the art would modify Ramasubramani with the disclosure of Mann. Ramasubramani fails to

disclose or suggest any type of deficiency within the art that would benefit from a modification that segments a message by a client device into a maximum segment size. Thus, the Examiner has fails to provide any deficiencies in Ramasubramani that would benefit from the alleged modification.

Moreover, the claims specifically recite a client device performing segmenting into a maximum segment size. The Examiner making general statements that Mann is not relied on to disclose that the client device is performing the segmenting is improper. The Applicants are **not** claiming as a general proposition segmenting. To the contrary, the Applicants are specifically claiming a client device segmenting a message into a maximum segment size. Respectfully, the Examiner is apparently ignoring an important feature of the claims, i.e., that it is a client device that is performing the segmenting into a message into a maximum segment size.

Moreover, the Examiner has failed to provide the desirability, as disclosed by Ramasubramani, for such a modification. The Examiner cites motivation from Mann for modifying Ramasubramani. However, it is the desirability of **modifying** Ramasubramani that is at issue, not the desirabillity of such use by Mann that discloses such a feature. Mann discloses the desirability of modifying a server, failing to disclose a desirability of modifying a client device. "The mere fact that the prior art may be modified in the manner suggested by the Examiner does not make the modification obvious unless the **prior art** suggested the desirability of the modification." In re Fritch, 23 USPQ2d 1780, 1783-84 (Fed. Cir. 1992). The Examiner has failed to provide the desirability of modifying Ramasubramani that makes sense within the context of the disclosure of Ramasubramani.

Neither Ramasubramani nor Mann disclose a client device performing segmenting into a maximum segment size (as acknowledged by the Examiner), much less disclose or suggest **modification of a client device** to perform segmenting into a maximum segment size, much less determining that at least one message segment constitutes a complete message by the client device and if the message segment constitutes a complete message as

determined the client device, transmitting from a protocol gateway to a message router the complete message, as recited by claims 12-18.

It is respectfully submitted that not only does this rejection fail on its face, but in view of the above comments its clear that claims 12-18 are not rendered obvious over Ramasubramani in view of Mann. Thus, the rejection of claims 12-18 under 35 U.S.C. § 103(a) over Ramasubramani in view of Mann is improper and should be reversed.

(E) Claims 20, 21, 25, 26, 30 and 31 are not obvious under 35 U.S.C. § 103(a) over Ramasubramani in view of Boyle and Attanasio.

Claims 20, 21, 25, 26, 30 and 31 require a method of routing and a message router authenticating an origin of a message before the message is routed by the message router between a protocol gateway and a server, a database accessible by the message router, and storing information relating to routing and authentication of the message.

As discussed above, Ramasubramani modified by the disclosure of Boyle fails to disclose, teach or suggest authenticating an origin of a message before the message is routed by a message router between a protocol gateway and a server, as recited by claims 20, 21, 25, 26, 30 and 31.

Attanasio is relied on to disclose load balancing across servers in a computer network (See Office Action dated August 4, 2004, page 27). Thus, even with a disclosure of load balancing across servers in a computer network, Ramasubramani modified by Boyle and Annasio still fails to disclose or suggest a method and apparatus authenticating an origin of a message before the message is routed by a message router between a protocol gateway and a server, as recited by claims 20, 21, 25, 26, 30 and 31.

Moreover, as discussed above, "Teachings of references can be combined only if there is some suggestion or incentive to do so." In re Fine, 5 USPQ2d 1596,1600 (Fed. Cir. 1988) (quoting ACS Hosp. Sys. v. Montefiore Hosp., 221 USPQ 929, 933 (Fed. Cir. 1984)) (emphasis in original). Modifying

Ramansubramani with the disclosure of Boyle and Attanasio, is **nonsensical**. The Examiner has not provided motivation why one of ordinary skill in the art would modify Ramansubramani in view of Boyle and Attanasio. Modifying Ramansubramani to authenticate an origin of a message before the message is routed by a message router between a protocol gateway and a server would serve no purpose within the context of Ramansubramani invention.

Thus, Ramansubramani modified by the disclosure of Boyle and Attanasio would still fail to disclose, teach or suggest a method and apparatus authenticating an origin of a message before the message is routed by a message router between a protocol gateway and a server, as recited by claims 20, 21, 25, 26, 30 and 31.

It is respectfully submitted that not only does this rejection fail on its face, but in view of the above comments its clear that claims 20, 21, 25, 26, 30 and 31 are not rendered obvious over Ramasubramani in view of Boyle, and further in view of Attanasio. Thus, the rejection of claims 20, 21, 25, 26, 30 and 31 under 35 U.S.C. § 103(a) over Ramasubramani in view of Boyle, and further in view of Attanasio is improper and should be reversed.

(F) Claims 36-41 are not obvious under 35 U.S.C. § 103(a) over Mann in view of Ramasubramani.

Claims 36-38 require a method of segmenting a message into one or more message segments by a client device, none of the message segments exceeding a maximum segment size, determining that at least one message segment constitutes a complete message by the client device and if the message segment constitutes a complete message as determined the client device, transmitting from a protocol gateway to a message router the complete message.

The Examiner acknowledges that Mann fails to disclose transmitting from a protocol gateway to a message router a complete message (See Office Action dated August 4, 2004, page 29). The Examiner relies on Ramasubramani to allegedly make up for the deficiencies in Mann to arrive at the recited features. The Applicants respectfully disagree.

The reason Mann fails to disclose transmitting from a protocol gateway to a message router a complete message (as acknowledged by the Examiner) is because Mann fails to disclose a gateway, much less a protocol gateway, much less transmitting from a protocol gateway to a message router a complete message, as recited by claims 36-41.

As discussed above, "Teachings of references can be combined only if there is some suggestion or incentive to do so." In re Fine, 5 USPQ2d 1596,1600 (Fed. Cir. 1988) (quoting ACS Hosp. Sys. v. Montefiore Hosp., 221 USPQ 929, 933 (Fed. Cir. 1984)) (emphasis in original). Modifying Mann with a protocol gateway, as disclosed by Ramansubramani, is **nonsensical**. The Examiner has not provided motivation why one of ordinary skill in the art would modify Mann with the disclosure of Ramasubramani. Mann fails to utilize a protocol gateway because a protocol gateway would serve no purpose in the system that does not require connection of networks having dissimilar protocols. Thus, modification of Mann would not cure any disclosed deficiencies that would benefit from the alleged modification.

The Examiner's motivation to modify Mann is that it would create a more robust and attractive system to users who wish to communicate with networks having different network characteristics (See Office Action dated August 4, 2004, page 30). However, the Examiner is modifying Mann with the disclosure of Ramansubramani, **not** Ramansubramani with the disclosure of Mann. Modifying Mann that lacks networks having different network characteristics with no need for a protocol gateway with a protocol gateway is **nonsensical**. Without a need for a protocol gateway, the Examiner has failed to detail how adding a protocol gateway to Mann would make the system more robust and attractive.

Moreover, as discussed above and as acknowledged by the Examiner, Mann fails to disclose segmenting a message into one or more message segments on a client device, as recited by claims 36-41.

Thus, Mann modified by the disclosure of Ramansubramani would fail to disclose, teach or suggest a method of segmenting a message into one or

more message segments on a client device, none of the message segments exceeding a maximum segment size, much less determining that at least one message segment constitutes a complete message by the client device and if the message segment constitutes a complete message as determined the client device, transmitting from a protocol gateway to a message router the complete message, as recited by claims 36-41.

Claims 39-41 require a method of defining a maximum segment size by a protocol gateway, segmenting a message into one or more message segments by the protocol gateway, none of the message segments exceeding a maximum segment size, and determining that at least one message segment constitutes a complete message by a client device.

The Examiner relies on Mann to disclose a server node defining a maximum segment size, a server node determining if the message exceeds the maximum segment size and a determining at a client device that at least one message segments constitutes a complete message (See Office Action dated August 4, 2004, page 31). The Examiner acknowledges that Mann fails to disclose a protocol gateway (See Office Action dated August 4, 2004, page 31). The Office Action relies on Ramansubramani to allegedly make up for the deficiencies in Mann to arrive at the claimed features. The Applicants respectfully disagree.

As discussed above, "Teachings of references can be combined only if there is some suggestion or incentive to do so." In re Fine, 5 USPQ2d 1596,1600 (Fed. Cir. 1988) (quoting ACS Hosp. Sys. v. Montefiore Hosp., 221 USPQ 929, 933 (Fed. Cir. 1984)) (emphasis in original). The Examiner alleges that it would have been obvious to have made the system of Ramansubramani more robust and attractive to users who wish to communicate with networks having different network characteristics (See Office Action dated August 4, 2004, page 31). However, the Examiner is modifying Mann to include a protocol gateway. Mann fails to rely on networks having different network characteristics for the implementation of Mann's invention. Thus, modifying Mann that fails to disclose networks having different network characteristics with a protocol

gateway that facilitates communications between networks having different network characteristics is **nonsensical**.

Moreover, the Examiner is relying on Ramansubramani to simply disclose a protocol gateway. However, even modifying Ramansubramani with a protocol gateway would still have Mann's server nodes performing any type of message segmenting based on a maximum segment size. Nothing within either Ramansubramani nor Mann discloses or suggests modifying a protocol gateway to define a maximum segment size and determine if a message exceeds a maximum segment size. Nothing within either Ramansubramani nor Mann discloses or **suggests** modifying Mann to remove the server nodes, replacing them with protocol gateways, and modifying the protocol gateways to have functions that were allegedly previously performed by the server nodes.

It is respectfully submitted that not only does this rejection fail on its face, but in view of the above comments its clear that claims 36-41 are not rendered obvious over Mann in view of Ramasubramani. Thus, the rejection of claims 36-41 under 35 U.S.C. § 103(a) over Mann in view of Ramasubramani is improper and should be reversed.

CONCLUSION

For all the reasons set forth above, the rejections of claims 1-41 are improper and should be reversed. The Applicants therefore respectfully request that this Appeal be granted and that the rejections of the claims be reversed.

Respectfully submitted,

William H. Bollman
Reg. No.: 36,457

MANELLI DENISON & SELTER PLLC
2000 M Street, N.W. 7th Floor
Washington D.C. 20036-3307
Tel. (202) 261-1020
Fax. (202) 887-0336

APPENDIX

CLAIMS INVOLVED IN THE APPEAL

1. A messaging system, comprising:

a client device having stored therein a client application adapted to be executed by said client device;

a server having stored therein a server application adapted to be executed by said server;

a plurality of wireless networks adapted to communicate messages between said client device and said server and support one or more wireless network protocols;

a protocol gateway to encapsulate a fundamental network protocol underlining each of said one or more wireless network protocols;

means for communicating a message between said client application and said server application, over a selected wireless network protocol through said protocol gateway, independent of said selected wireless network protocol; and

a message router for routing said message between said protocol gateway and said server, said message router including:

means for authenticating an origin of said message, wherein said authenticating means authenticates said origin before said message is routed by said message router; and

a database accessible by said message router and adapted to store information relating to routing and authentication of said message.

2. The messaging system according to claim 1, further comprising:

a simple network transport layer application adapted to be executed by said protocol gateway and including a first code segment for defining a maximum segment size, a second code segment for determining if said message exceeds said maximum segment size, and a third code segment for segmenting said message into a plurality of message segments, none of said message segments exceeding said maximum segment size.

3. The messaging system according to claim 2, further comprising:

means for supporting a message retry in each of said wireless network protocols.

4. The messaging system according to claim 2, further comprising:

means for supporting a message ACK/NACK service in each of said wireless network protocols.

5. A method of communicating a message over a plurality of wireless networks between a client device having stored therein a client application adapted to be executed by the client device and a server having stored therein a server application adapted to be executed by the server, each of said plurality of wireless networks is adapted to support one or more wireless network protocols, said method comprising the steps of:

providing a remotely manageable protocol gateway;

encapsulating a fundamental network protocol by said protocol gateway, said fundamental network protocol underlies each of said one or more wireless network protocols communicating said message between said client application and said server application over a selected wireless network protocol through said remotely manageable protocol gateway independent of said selected wireless network protocol; and

providing a message router for routing said message between said remotely manageable protocol gateway and said server.

6. The method according to claim 5, further comprising:

authenticating an origin of said message.

7. The method according to claim 6, wherein:

said authenticating step is performed by said message router before said message is routed between said remotely manageable protocol gateway and said server.

8. The method according to claim 6, further comprising:

providing a database accessible by said message router; and

storing in said database information relating to routing and authentication of said message.

9. The method according to claim 5, further comprising:

providing a simple network transport layer (SNTL) application, wherein said SNTL application is adapted to be executed by said remotely manageable protocol gateway;

defining a maximum segment size;

determining if said message exceeds said maximum segment size; and

segmenting said message into a plurality of message segments, none of said message segments exceeding said maximum segment size.

10. The method according to claim 5, further comprising:

supporting a message retry in each of said wireless network protocols.

11. The method according to claim 5, further comprising:

supporting a message ACK/NACK service in each of said wireless network protocols.

12. A method of routing a message in a communications system, comprising:

providing a server adapted to run a server application;

providing a plurality of message routers coupled to said server;

providing a plurality of protocol gateways coupled to each one of said plurality of message routers; and

providing a wireless network adapted to couple said server through one or more of said plurality of message routers and one or more of said plurality of protocol gateways to a plurality of client devices, each of said client devices adapted to run a client application;

transmitting said message from one of said plurality of client devices:

defining a maximum segment size by said one of said plurality of client devices;

determining if said message exceeds said maximum segment size by said one of said plurality of client devices;

segmenting said message into one or more message segments by said one of said plurality of client devices, none of said message segments exceeding said maximum segment size;

receiving said message at one of said plurality of protocol gateways;

transmitting from said one of said plurality of protocol gateways to said one of said plurality of client devices a first acknowledgment message acknowledging receipt of at least one message segment by said one of said plurality of protocol gateways;

determining that said at least one message segment constitutes a complete message by said one of said plurality of client devices;

if said at least one message segment constitutes a complete message as determined by said one of said plurality of client devices, transmitting from said one of said plurality of protocol gateways to one of said plurality of message routers said complete message; and

routing said complete message to said server by said one of said plurality of message routers.

13. The method according to claim 12, further comprising:

transmitting from said server to said one of said plurality of message routers a second acknowledgment message acknowledging receipt of at least one message segment by said one of said plurality of protocol gateways;

receiving said second acknowledgment message at said one of said plurality of message routers and routing said second acknowledgment message to said one of said plurality of protocol gateways;

receiving from said one of said plurality of message routers said second acknowledgment message at said one of said plurality of protocol gateways; and

transmitting said second acknowledgment message from said one of said plurality of protocol gateways to said one of said plurality of client devices transmitting said message.

14. The method according to claim 12, wherein:

if a size exceeds said maximum segment size, segmenting said message into a first message segment and a second message segment, neither of said first message segment and said second message segment exceeds said maximum segment size;

transmitting from said one of said plurality of protocol gateways to said one of said plurality of client devices a first acknowledgment message acknowledging receipt of said first message segment by said one of said plurality of protocol gateways;

receiving said first acknowledgment message at said one of said plurality of client devices;

determining by said one of said plurality of client device that said second message segment was not received by said one of said plurality of protocol gateways;

retransmitting from said one of said plurality of client devices to said one of said plurality of protocol gateways said second message segment; and

receiving said retransmitted second message segment at said one of said plurality of protocol gateways; and

transmitting from said one of said plurality of protocol gateways to said one of said plurality of client devices a second acknowledgment message acknowledging receipt of said second message segment by said one of said plurality of protocol gateways.

15. The method according to claim 14, further comprising:

determining by said one of said plurality of protocol gateways that said first message segment and said second message segment comprises a complete message; and

transmitting a complete message acknowledgment message from said one of said plurality of protocol gateways to said one of said plurality of client devices upon receipt of said retransmitted second message segment by said one of said plurality of protocol gateways.

16. A method of routing a message in a communications system, comprising:

providing a server adapted to run a server application;

providing a plurality of message routers coupled to said server;

providing a plurality of protocol gateways coupled to each one of said plurality of message routers; and

providing a wireless network adapted to couple said server through one or more of said plurality of message routers and one or more of said plurality of protocol gateways to a plurality of client devices, each of said client devices adapted to run a client application;

transmitting said message from said server to one of said plurality of message routers;

receiving said message at said one of said plurality of message routers, and routing said message to one of said plurality of protocol gateways;

defining a maximum segment size by said one of said plurality of protocol gateways;

determining if said message exceeds said maximum segment size by said one of said plurality of protocol gateways;

segmenting said message into one or more message segments by said one of said plurality of protocol gateways, none of said message segments exceeds said maximum segment size;

receiving said message at one of said plurality of protocol gateways;

transmitting said message from said one of said plurality of protocol gateways to said one of said plurality of client devices;

receiving said message at said one of said plurality of client devices;

transmitting an acknowledgment message from said one of said plurality of client devices to said one of said plurality of protocol gateways, said acknowledgment message acknowledges receipt of at least one message segment by said one of said plurality of client devices; and

determining that said at least one message segment constitutes a complete message by said one of said plurality of client devices.

17. The method according to claim 16, wherein:

if a size exceeds said maximum segment size, segmenting said message into a first message segment and a second message segment by said one of said plurality of protocol gateway, neither of said first message segment and said second message segment exceeds said maximum segment size;

transmitting from said one of said plurality of protocol gateways to said one of said plurality of client devices said first message segment and said second message segment;

receiving said first message segment at said one of said plurality of client devices;

transmitting from said one of said plurality of client devices to said one of said protocol gateways a first acknowledgment message acknowledging receipt of said first message segment by said one of said plurality of client devices;

determining that said second message segment was not received by said one of said plurality of client devices by said one of said plurality of protocol gateways;

retransmitting from said one of said plurality of protocol gateways to said one of said plurality of client devices said second message segment;

receiving said retransmitted second message segment at said one of said plurality of client devices; and

transmitting from said one of said plurality of client devices to said one of said plurality of protocol gateways a second acknowledgment message, said second acknowledgment message acknowledges receipt of said second message segment by said one of said plurality of client devices.

18. The method according to claim 16, further comprising:

determining by said one of said plurality of protocol gateways that said first message segment and said second message segment comprises a complete message; and

transmitting a complete message acknowledgment message from said one of said plurality of protocol gateways to said one of said plurality of client devices upon receipt of said retransmitted second message segment by said one of said plurality of client devices.

19. A message router for routing a message between a protocol gateway and a server, the message router comprising:

an authenticator to authenticate an origin of said message, said authenticator authenticating said origin of said message before said message is routed by said message router between a protocol gateway and a server; and

a database accessible by said message router and adapted to store information relating to routing and authentication of said message.

20. The message router according to claim 19, wherein:

said message is routed to a least recently used protocol gateway.

21. The message router according to claim 19, wherein:

said message is routed to said message router if said message router is a least recently used message router.

22. The message router according to claim 19, wherein:

said message router routes said message to a most specific server corresponding to a message key.

23. The message router according to claim 19, wherein:

said message router routes said message based on a content of said message.

24. A method of routing a message between a protocol gateway and a server comprising:

authenticating an origin of said message before said message is routed by said message router between a protocol gateway and a server;

accessing a database by said message router; and

storing information relating to routing and authentication of said message.

25. The method of routing a message according to claim 24, further comprising:

routing said message to a least recently used protocol gateway.

26. The method of routing a message according to claim 24, further comprising:

routing said message to said message router if said message router is a least recently used message router.

27. The method of routing a message according to claim 24, further comprising:

routing said message to a most specific server corresponding to a message key.

28. The method of routing a message according to claim 24, further comprising:

routing said message based on a content of said message.

29. An apparatus for routing a message between a protocol gateway and a server comprising:

means for authenticating an origin of said message before said message is routed by said message router between a protocol gateway and a server;

means for accessing a database by said message router; and

means for storing information relating to routing and authentication of said message.

30. The apparatus for routing a message according to claim 29, further comprising:

means for routing said message to a least recently used protocol gateway.

31. The apparatus for routing a message according to claim 29, further comprising:

means for routing said message to said message router if said message router is a least recently used message router.

32. The apparatus for routing a message according to claim 29, further comprising:

means for routing said message to a most specific server corresponding to a message key.

33. The apparatus for routing a message according to claim 29, further comprising:

means for routing said message based on a content of said message.

34. A system for communicating a message over a plurality of networks between a client device and a server comprising:

said client device to execute a client application;

said server to execute a server application; and

a remotely manageable protocol gateway to encapsulate a fundamental network protocol underlying each of a plurality of network protocols communicating said message between said client application and said server application over a selected wireless network protocol through said remotely manageable protocol gateway independent of said selected wireless network protocol.

35. The system for communicating a message over a plurality of networks between a client device and a server, according to claim 34 further comprising:

a message router to route a message between said client application and said server application, said message router located between said remotely manageable protocol gateway and said server.

36. A method of routing a message in a communications system, comprising:

defining a maximum segment size by a client device;

determining if a message exceeds a maximum segment size by said client device;

segmenting said message into one or more message segments by said client device, none of said message segments exceeding said maximum segment size; and

if said message segment constitutes a complete message as determined said client device, transmitting from protocol gateways to a message router said complete message.

37. The method according to claim 36, further comprising:

if a size exceeds said maximum segment size, segmenting said message into a first message segment and a second message segment, neither of said first message segment and said second message segment exceeds said maximum segment size.

38. The method according to claim 37, further comprising:

determining by said protocol gateway that said first message segment and said second message segment comprises a complete message.

39. A method of routing a message in a communications system, comprising:

defining a maximum segment size by a protocol gateway;

determining if a message exceeds a maximum segment size by said protocol gateway;

segmenting said message into one or more message segments by said protocol gateway, none of said message segments exceeding said maximum segment size; and

determining by said client device that said message segment constitutes a complete message.

40. The method according to claim 39, further comprising:

if a size exceeds said maximum segment size, segmenting said message into a first message segment and a second message segment, neither of said first message segment and said second message segment exceeds said maximum segment size.

41. The method according to claim 40, further comprising:

determining by said protocol gateway that said first message segment and said second message segment comprises a complete message.